DEPARTMENT: HealthTrust Ethics and Compliance	**POLICY DESCRIPTION:** PHI: Avoiding Protected Health Information
PAGE: 1 of 9	**REPLACES POLICY DATED:** n/a
EFFECTIVE DATE: May 25, 2016	**REFERENCE NUMBER:** HT.021
APPROVED BY: HealthTrust Ethics and Compliance Committee	

SCOPE: All departments within HealthTrust Purchasing Group, L.P. ("HealthTrust LP"); Invivolink LLC; and to the extent applicable, direct and indirect subsidiaries or affiliates of HealthTrust LP (including HealthTrust-Europe LLP and the representative office of HealthTrust in Shanghai – see Policy 2; and provided that no shareholder of HCA Holdings, Inc. shall be deemed to be an affiliate) (collectively, "HealthTrust").

PURPOSE: To ensure that all HealthTrust Colleagues understand what is required to avoid receiving or retaining Protected Health Information ("PHI") when not necessary for a Client engagement, in accordance with the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), the Privacy Standards, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") component of the American Recovery and Reinvestment Act, related regulations and guidelines, and applicable state laws. To ensure all HealthTrust Colleagues understand what actions must be taken if unnecessary PHI is received.

DEFINITIONS: Capitalized terms are defined. See back pages of this policy.

ESSENTIAL INFORMATION: ***This is a summary of selected topics and definitions. Please read this entire document for full information.***

1. Compliance with laws relating to PHI. All Colleagues must be trained to comply with laws relating to Protected Health Information ("PHI"). HealthTrust may access, use and disclose PHI only for a proper purpose under HIPAA, the Client's Business Associate Agreement ("BAA") and company privacy policies. If a Colleague accesses, uses or discloses PHI for a purpose other than a proper purpose, it could be a violation of law. All Colleagues must take reasonable steps to protect PHI from any impermissible access, use or disclosure. They may access, use and disclose only the minimum necessary type and quantity of PHI required to perform their assignments.

2. What is PHI? PHI is any individually-identifiable Health Information. Health Information includes any information that relates to the past, present or future physical or mental condition of an individual. See Exhibit A for a list of the "identifiers". Some are easily recognizable as data that could lead to a person's identity such as name, phone number, address or certain demographic information. Other identifiers are less obvious, such as an account number.

3. Avoiding PHI. If PHI is not required for a Client engagement, Colleagues must ensure that PHI is either not received by HealthTrust or is rejected or securely destroyed if received, as soon as reasonably practicable. If PHI is required, Policy HT.022 must be followed.

4. Department Privacy Manager ("DPM"). Each executive in charge of a working group that receives Client data must ensure the group has a DPM. The DPM ensures compliance with this policy within the group.

5. Is PHI necessary for this project? Minimum necessary standard. HIPAA requires that HealthTrust and the Covered Entity determine what information is necessary for the Client engagement. The working group must strive to carry out the engagement without receiving PHI. If PHI is required, Policy HT.022 must be

followed instead of this policy.

6. Request for and review of data. For each Client engagement for which PHI is not needed, HealthTrust and the Client will agree on what data is needed, and HealthTrust will communicate with the Client requesting just the specified data and asking the Client not to provide any PHI. The data is reviewed on receipt to see if it conforms. If it contains PHI, the Client is informed and reminded exactly what data is needed. Other steps may include purging and resending the data; masking or deleting PHI; or denial of Colleagues' access until the PHI is removed.

7. Documentation. For working groups that have no need to receive PHI yet occasionally receive it, documentation must be maintained to evidence proper handling of such incidents. The DPM, with senior leadership in the DPM's group, shall determine the specific format of a Log to be maintained by the Department, and any other required documentation.

8. Ramifications. If PHI is received as described above, it is not a non-permitted access or use by HealthTrust, and it is not a Security Incident. HealthTrust shall cooperate fully with the Client in investigating and mitigating any such issue. Similarly, it is not a "reportable issue" under company policy.

9. Receipt of PHI by mistake. Some Colleagues may receive PHI by mistake under circumstances not related to their role at HealthTrust. In such a case, the Colleague should notify the sender.

10. Sanctions. Sanctions may be imposed against Colleagues who fail to comply with this policy, Policy HT.022 or other company privacy policies.

11. Reporting. If a Colleague knows of, suspects or has received a report from any person of a violation or potential violation of this policy, Policy HT.022 or other company privacy policies by a Colleague or a HealthTrust contractor, he or she must immediately notify the ECO or the Ethics Line at 1-800-345-7419. (See the Code of Conduct for numbers and dialing instructions for the U.K. and China.)

POLICY

1. Compliance with laws relating to PHI. All Colleagues must be trained to comply with laws relating to proper handling of PHI. The HealthTrust Ethics and Compliance Officer ("ECO") shall ensure that all applicable Colleagues receive regular training on this policy, and that this policy is updated and employees trained on any material changes to laws affecting this policy. Training should occur within a reasonable period of time after a Colleague joins the workforce, and after a material change in law. Documentation of training must be maintained per Procedure 16 of Policy HT.022.

2. Access to, use and disclosure of PHI only for a "proper purpose". HealthTrust may access, use and disclose PHI only as necessary and permitted by law, the Client's BAA and other company policies. Such access, use

or disclosure must be for a proper purpose under HIPAA, including Healthcare Operations or Payment (see Definitions). The term "Healthcare Operations" includes many services that HealthTrust may provide to a Client such as administrative, legal, financial and quality improvement activities. If a Colleague accesses, uses or discloses PHI for a purpose other than a proper purpose under HIPAA, it could be a violation of law. If you intend to send PHI to a location outside of the United States, or if you receive patient information from a source outside the United States, contact the ECO.

3. Protecting PHI. All Colleagues must take reasonable steps to protect PHI from any impermissible access, use or disclosure. If PHI is required, Policy HT.022 and company policies relating to the Security Standards must be followed.

4. Avoiding PHI. If PHI is not required for a Client engagement, Colleagues must ensure that PHI is either not received by HealthTrust or is rejected or destroyed if received, as soon as reasonably practicable.

PROCEDURE

1. What is PHI? PHI or Protected Health Information means any oral, written or electronic individually-identifiable Health Information. It includes demographic information and information relating to the past, present or future physical or mental condition of an individual. See Exhibit A for factors that can make such information individually identifiable. Some identifiers are easily recognizable as data that could lead to a person's identity such as name, phone number or address. Other identifiers are less obvious, such as an account number. To be PHI, an identifier must be connected to the Health Information. This too can be less than obvious. For example if we have P.O. information showing that a knee was purchased, we know the patient had a knee replacement (Health Information). If identifiers are also present, we have PHI.

2. PHI within HealthTrust. HealthTrust has two main policies relating to PHI, in addition to policies relating to the Security Standards for PHI:
   - This Policy HT.021 – *PHI: Avoiding Protected Health Information* addresses Client engagements for which access to PHI is not necessary. It contains guidance for avoiding the receipt of PHI, and describes what to do if unnecessary PHI is received.
   - Policy HT.022 – *PHI: Managing Protected Health Information* addresses Client engagements for which access to PHI is necessary, and sets out requirements for proper handling and protection of PHI.

3. Department Privacy Manager ("DPM") role.
   a. Appointment. Each executive in charge of a working group that receives Client data must ensure that the group has a DPM. The DPM may delegate tasks but remains responsible for ensuring compliance within the group with this policy. If a Colleague does not know the identity of his or her DPM, or if a DPM is unsure as to what working group(s) he or she supports, contact the ECO.
   b. Responsibilities. These are the key responsibilities of the DPM under this policy:
      i. Ensure that PHI is managed within the working group in compliance with this policy, working with the business team, the Director of Information Security Assurance ("DISA"), the Legal Department,

the ECO and others as needed;

ii. Where PHI is not needed for an engagement, work with the group to ensure that all appropriate communications to Clients emphasize that PHI is not needed and retain the related documentation;

iii. Report to the ECO any actual or potential inappropriate access, use or disclosure of PHI or any actual or potential Security Incident on the day the DPM discovers or is made aware of the incident; report to the ECO as soon as possible any activity of which the DPM is aware, that may constitute or result in a violation of this policy or other company privacy policies;

iv. Work with the ECO to investigate and resolve incidents relating to PHI and privacy matters; and

v. Implement within the group steps necessary to mitigate issues caused by any violation or risk of violation of this policy.

c. DPMs that serve in a supporting role. Some DPMs are in a working group that serves in a supporting role; for example, the Legal Department; IT&S staff responsible for data storage, access controls and physical security; and in some cases the Finance and Accounting Support group that reports to the CFO and is not connected to a line of business. These groups may receive PHI to store or secure it, or review a legal, financial or accounting issue, but they do not analyze PHI or work with it to create analytic or other tools, aggregate such data, or otherwise work with PHI. DPMs for those groups may not need to comply with all DPM requirements in this policy if another DPM whose group works directly with such data is the more appropriate person to do so. In such case the DPMs must work together to ensure that all DPM requirements are met, with the DISA ensuring that Security Standards are met.

4. Is PHI necessary for this project? Minimum necessary standard. HealthTrust must not use, disclose or request any PHI unless it is necessary to carry out a Client engagement. The DPM will enforce this standard within the working group by considering the following criteria for each proposed access, use or disclosure of Client data, to assess whether PHI is needed:

- What is the purpose of the proposed access, use or disclosure of Client information?
- If PHI is needed, what type of PHI is needed for the stated purpose?
- Are there reasonable alternatives to using PHI (for example using De-identified Information)?
- Are there any other factors relevant to the requested access, use or disclosure?

The DPM and others in the working group must strive to carry out the engagement without receiving any PHI if possible. If PHI is required, Policy HT.022 must be followed instead of this policy. If PHI is not required, actions described in this policy must be taken to ensure that (i) PHI is not received, or (ii) if PHI is received, it is handled as described in this policy.

5. Prevention first! The request for data.

a. Planning stage. For each Client engagement for which PHI is not needed, HealthTrust and the Client must agree on what data is needed. A Colleague will send an email substantially in the form of Exhibit C, or another form of communication, advising the Client as to specific types of data needed, and

asking the Client not to provide any PHI.

b. Outsourced Colleagues. Colleagues who are outsourced to work at a Client facility must never put Client PHI into a HealthTrust system without the prior written approval of the CEO, CMO or COO, copy to the ECO. Such Colleagues should ensure wherever possible that the Client manages their access and prevents their access to PHI through roles-based controls.

c. De-identified Information; Limited Data Sets. If reasonably practical, PHI should be "De-identified" by the Client (or by HealthTrust if permitted under the Client's BAA) substituting a code for the PHI. De-identified data is no longer PHI and may be used in any manner permitted under agreements between HealthTrust and the Client. Limited Data Sets should also be considered and used if practicable. Limited Data Sets are still considered to be PHI since they contain some identifiers. See Policy HT.022 for more information.

6. Review of data.
   a. Preliminary review of data. Upon receipt of the data or accessing it on the Client's system, HealthTrust must take reasonable steps to review it to see if the data contains any PHI. This can be done by one Colleague for the entire working group, or by individual Colleagues.

   b. If the data contains PHI. If a Colleague finds that the data contains PHI, the DPM and the Client must be contacted as soon as possible to determine next steps. The HealthTrust relationship manager for the Client should also be contacted. HealthTrust must reiterate for the Client exactly what data is needed. Other steps may include purging and reloading or resending the data; masking or deleting the PHI; or denial of Colleagues' access until the PHI is removed. If a Colleague discovers PHI in the file after he or she has put several hours work into it, contact the DPM to see if deletion of the file can be avoided. If the Client insists on sending PHI, contact the Legal Department. If a Colleague is unsure if a data set contains PHI, it should be investigated in a way that does not transmit additional copies of the data. Describe the suspected PHI to the DPM rather than emailing the data.

   c. Documentation. For working groups that have no need to receive PHI yet occasionally receive it, documentation must be maintained to evidence proper handling of such incidents. The DPM shall determine the specific format of a Log to be maintained by the Department and any other required documentation. A form of Log is attached as Exhibit B, which may be adapted to better fit the group's circumstances. The Log and other documentation shall be retained for six years from the date of the last entry into the Log, or six years from the date of creation of the other documentation, as applicable.
   d. Ramifications. If HealthTrust or a Colleague receives PHI as part of the process described in this Procedure 6, it is not a non-permitted access or use by HealthTrust and is not a Security Incident because it occurs in the context of HealthTrust's good faith effort to carry out the Client engagement in compliance with law. Thus, it is not required to be reported under Procedure 11(d) of Policy HT.022. In such case HealthTrust shall cooperate fully with the Client in compliance with its BAA in investigating

and mitigating any such issues. Similarly, it is not a "reportable issue" under company policy.

7. Receipt of PHI by mistake. Some Colleagues may receive PHI by mistake under circumstances not related to their role at HealthTrust. For example one Colleague's HealthTrust fax number is similar to that of a local physician, and another Colleague's name is similar to that of a clinician at a member hospital. In each instance, these Colleagues have had PHI misdirected to them. In such a case, notify the sender for direction as to how to respond and to avoid a recurrence.

8. Sanctions. Sanctions may be imposed against Colleagues who fail to comply with this policy, Policy HT.022 or other company privacy policies. See Procedure 14 of Policy HT.022.

9. Reporting. If any Colleague knows of, suspects or receives a report from any person of a violation or potential violation of this policy, Policy HT.022 or other company privacy policies by a Colleague or a HealthTrust contractor, he or she must notify the ECO or the Ethics Line at 1-800-345-7419. (See the Code of Conduct for numbers and dialing instructions for the U.K. and China.) An actual or potential impermissible access, use or disclosure of PHI must be reported on the day the matter is discovered. Other incidents should be reported as soon as possible. HealthTrust will not intimidate, threaten, coerce or retaliate against a person who reports a matter under this policy or participates in a related investigation.

The ECO is responsible for overseeing the implementation of this policy. For questions, please contact Lynn Egan at 615-344-3947, Lynn.Egan@HealthTrustpg.com.

DEFINITIONS

Business Associate means a person, business or other entity who, on behalf of a Covered Entity, creates, receives, maintains, or transmits PHI, for a function or activity regulated by HIPAA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and re-pricing; or provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another business associate of such Covered Entity or arrangement, to the person. A business associate is not someone in a facility's own workforce, such as an employee, volunteer, or trainee.

Business Associate Agreement ("BAA") means an agreement with a Business Associate and HealthTrust or another third party that contains terms required by 45 CFR §164.504, including how PHI may be used or disclosed and requiring the maintenance of safeguards for PHI.

CEO means the chief executive officer of HealthTrust.

CFO means the chief financial officer of HealthTrust.

Client means a member of the HealthTrust GPO and/or a customer or client of HealthTrust that receives fee-based consulting services (and in some cases assistance with custom contracting) offered by HealthTrust.

CMO means the chief medical officer of HealthTrust.

Colleague or HealthTrust Colleague means any individual who works full- or part-time for HealthTrust including
(i) employees of HealthTrust,
(ii) employees of HCA Management Services, L.P. who work for HealthTrust under a management contract,
(iii) employees of China International Intellectech (Shanghai) Corporation who are dispatched to work for the Shanghai Office, or
(iv) independent contractors providing services to HealthTrust.

Covered Entity means a health plan (*e.g.*, an individual or group plan that provides or pays the cost of medical care), a health care clearinghouse, or a health care provider that transmits any health information in connection with a transaction covered by HIPAA.

De-identified Information means information that does not include any of the following identifiers of an individual or the individual's employer, family members or household members: name; all geographic subdivisions smaller than a state (including street address, city, county, precinct and zip code); all elements of dates related to an individual (including birth date, admission date and discharge date) except for years (other than year of birth for those over 89); telephone numbers; fax numbers; electronic mail address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; serial number of a vehicle or other device identifier; internet URL; internet protocol (IP) address number; biometric identifiers, including finger and voice prints; full face photographic images and any other unique information that could reasonably be used alone or in combination with other information to identify an individual.

DISA means HealthTrust's Director of Information Security Assurance whose role is described in HCA Policy IP.SEC.006 - *Information Security Roles and Responsibilities*.

DPM or **Department Privacy Manager** means the person responsible for ensuring compliance within his or her department with this policy, Policy HT.022 and any other policies issued by HealthTrust relating to PHI or other privacy matters.

ECO means the Ethics and Compliance Officer of HealthTrust LP reporting directly to the CEO.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Healthcare Operations means certain administrative, financial, legal and quality improvement activities of a health care provider that are necessary to run its business and to support treatment and payment. HealthTrust may assist a Client with some of these activities, including but not limited to the following:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, customer service, creating De-identified health information or a Limited Data Set.

HIPAA means the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (**Privacy Standards**) the Standards for Breach Notification for Unsecured Protected Health Information (**Breach Notification Standards**), and the Security Standards for the Protection of Electronic Protected Health Information (**Security Standards**). For ease of reference, herein the term is also deemed to include the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009.

Limited Data Set means PHI that excludes the following identifiers of the patient and the patient's relatives, employers and household members: names, postal address, telephone number, fax number, e-mail address, social security number, medical record number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers, device identifiers, web universe resource locators, internet protocol address numbers, biometric identifiers, including finger and voice prints, and full face photographic images.

Log means the log described at Procedure 6(c) herein.

Payment means various activities of health care providers to obtain payment or be reimbursed for their services, and to obtain or provide reimbursement for provision of health care. The HIPAA rule provides examples of common payment activities including but not limited to: determining eligibility or coverage under a plan and adjudicating claims; risk adjustments; billing & collection activities; reviewing health care services for medical necessity, coverage, justification of charges, and the like; utilization review activities; disclosures to consumer reporting agencies (limited to specified identifying information about an individual, his or her payment history, and identifying information about the Covered Entity).

PHI or **Protected Health Information** means any oral, written or electronic individually-identifiable health information collected or stored by a Covered Entity. Individually-identifiable health information includes demographic information and any information that relates to the past, present or future physical or mental condition of an individual. Identifiers that can render such information individually identifiable are listed on Exhibit A.

Policy HT.022 means HealthTrust Policy HT.022 – *PHI: Managing Protected Health Information.*

Privacy Standards means the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

DEPARTMENT: HealthTrust Ethics and Compliance	POLICY DESCRIPTION: PHI: Avoiding Protected Health Information
PAGE: 9 of 9	**REPLACES POLICY DATED:** n/a
EFFECTIVE DATE: May 25, 2016	**REFERENCE NUMBER:** HT.021
APPROVED BY: HealthTrust Ethics and Compliance Committee	

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Standards means the security standards for the Protection of Electronic PHI under HIPAA. 45 C.F.R. Part 160 and Part 164, Subparts A and C. These standards are managed by the DISA.

Unsecured Protected Health Information or Unsecured PHI means PHI that is not encrypted or rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the U.S. Secretary of Health and Human Services.

REFERENCES:

HealthTrust Code of Conduct
Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Reinvestment and Recovery Act of 2009, Title XIII, Subtitle D
Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E
Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and C
Standards for Breach Notification for Unsecured Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and D
Policy HT.022 – *PHI: Managing Protected Health Information*

HT.021 PHI: Avoiding Protected Health Information

Exhibit A

Patient "Identifiers" under HIPAA
that constitute PHI
if combined with "Health Information"

Identifiers:

• Name • Address including street, city, county, zip code • All elements (except year) of dates related to an individual (including day and month of birth, admission /discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax numbers • Email addresses • Social security number	• Medical record number • Health plan beneficiary number • Account number • Certificate/license number • Any vehicle identifiers and serial numbers, including license plate • Medical device identifiers and serial numbers • Web universal resource locator (URL) • Internet protocol address (IP) • Finger or voice prints • Full face photographic images & any comparable images • Any other unique identifying number

Health Information:

means any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to:

- the past, present, or future physical or mental health or condition of an individual;
- the provision of health care to an individual; or
- the past, present, or future payment for the provision of health care to an individual.

HT.021 PHI: Avoiding Protected Health Information

Exhibit B

Sample Log for Recording Receipt and Disposition of Unnecessary PHI

Date unneeded PHI received	Client name	Facility name	Colleague(s) who rec'd it	Format (email, excel, data feed, etc.)	HT system name (*e.g.* Insight)	Details of incident	Action taken	Date action taken	Comments

HT.021 PHI: Avoiding Protected Health Information

Exhibit C
Email template for use in requesting data from Clients (NO PHI)

To: Client**;** **From**: [name], HealthTrust; **Subject**: Data for HealthTrust analysis

We at HealthTrust are very pleased to have the opportunity to [describe engagement] for [client]. I enclose an Excel spreadsheet that indicates types of data that HealthTrust requires to perform the analyses you have requested.

We are very vigilant as to client confidential information, particularly information that may constitute protected health information, or PHI. As you know, PHI consists of information relating to the physical or mental health or condition of an individual, the provision of health care, or payment for same, plus any one of the identifiers set out on Attachment 1 to this email.

To carry out the analyses that we have discussed, HealthTrust does NOT require any PHI from your organization. Please do not send or provide access to any information that could constitute PHI. We hope to complete this work as soon as we possibly can, and if you provide PHI, it will result in delays. If you have questions about whether particular types of data constitute PHI, please contact your organization's privacy or ethics officer.

[Use this paragraph if client will send data in an Excel file]: Please populate the spreadsheet with the requested data, carefully avoiding inclusion of any PHI. [Add specifics - is to be emailed or loaded by the Client onto a server?] If PHI is sent to HealthTrust, our policy requires that we delete the file and request that you send a file that does not contain PHI.

[Use this paragraph if client will make the data available by providing HealthTrust Colleagues with access to the Client's computer systems.]: Please get back to me with the details for granting access for certain HealthTrust employees to your hospital's computer systems to review the necessary data, doing your best to ensure that PHI will not be accessible to them. If accessing PHI on your systems will be unavoidable, please contact me so that we can ensure that appropriate protections are in place and a **Business Associate Agreement** is signed prior to our accessing the data.

Attachment 1 to email: Any one of these patient "Identifiers" plus "Healthcare Information" = PHI

• Name • Address including street, city, county, zip code • All elements (except year) of dates related to an individual (including day and month of birth, admission/discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax numbers • Email addresses • Social security number • Medical record number	• Health plan beneficiary number • Account number • Certificate/license number • Any vehicle identifiers and serial numbers, including license plate • Medical device identifiers and serial numbers • Web universal resource locator (URL) • Internet protocol address (IP) • Finger or voice prints • Full face photographic images & any comparable images • **Any other unique identifying number**